Режим поверки зондов WPE-103 и WPE-108

Режим поверки реализован для осуществления поверки измерительным комплексом «ВЕКТОР ИКИ».или "АМУЛЕТ"(в случае однопортового зонда sheeva)

Реализация

Проверка прибором "ВЕКТОР ИКИ" Реализована с помощью iptables и утилиты ulog-acctd. Проверка "АМУЛЕТ" использует "сырые" сокеты для получения данных о переданной информации на зонд.

Для осуществления поверки добавлен новый режим **verification** в пользовательский telnet. Для того чтобы зайти в этот режим, необходим обладать правами, не ниже admin. Переключение в режим поверки происходит из режима конфигурации, при вводе verification.

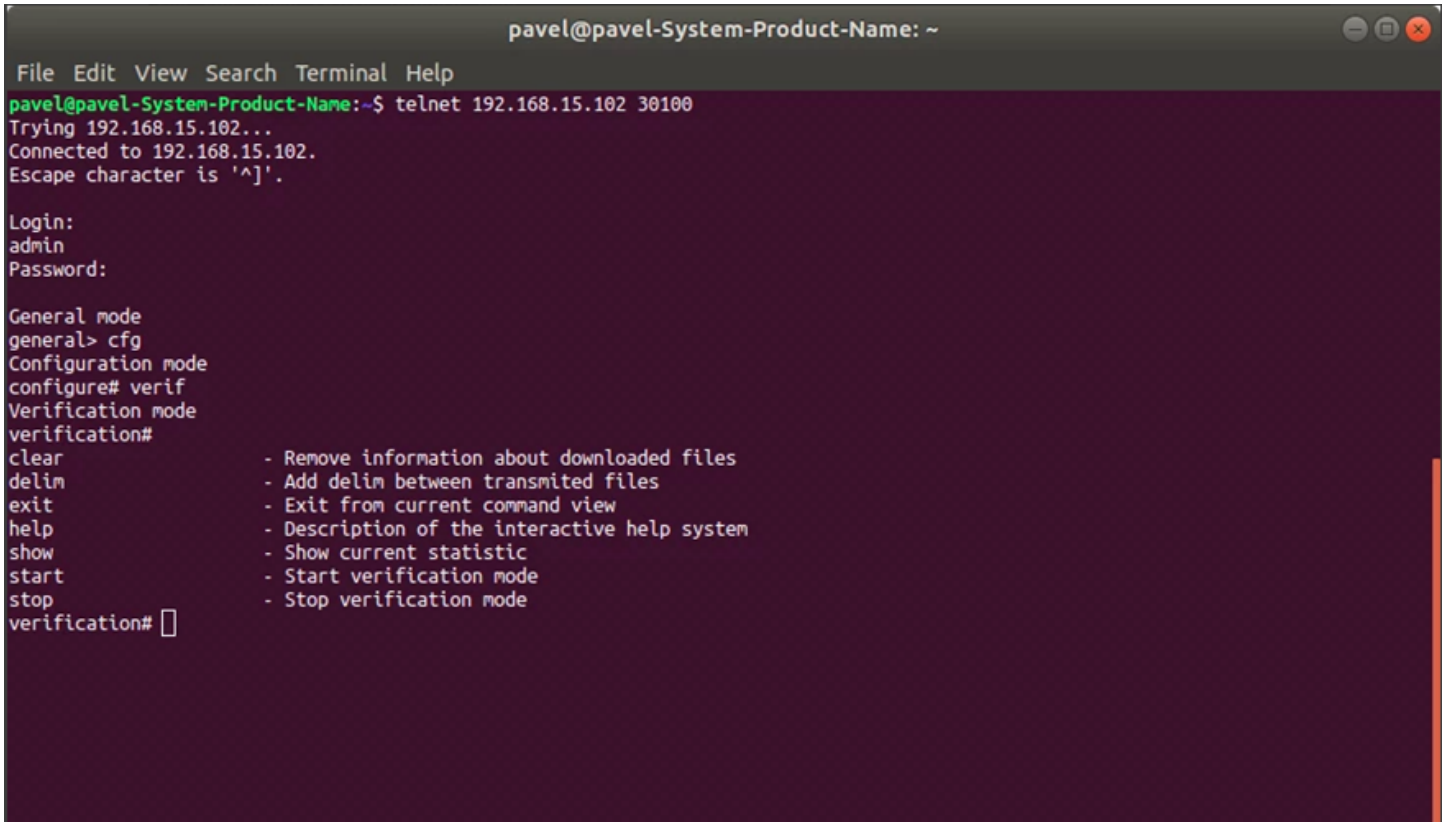


Рисунок 67 — Список команд в режиме поверки

Описание команд

- clear — записывает вектор информации о переданных файлах в текстовый документ (/var/log/slamon.%Y%m%d-%H-%M-%S). Затем очищает вектор, в котором содержится.

- delim — выполняется после успешной отправки файла. Подсчитывает количество переданной информации, количество пакетов и среднюю скорость.
- exit — осуществляет выход из режима поверки.
- help — открывает описание интерактивной справочной системы.
- show — выводит информацию на текущий момент.
- start — запускает wizard и подготавливает устройство к поверке. Подробнее в «Выполнение поверки».
- stop — останавливает поверку и возвращает устройство в «обычный» режим работы.

Выполнение поверки

После ввода команды «`start`», «wizard» запрашивает данные от пользователя в зависимости от собранной схемы:

Рисунок 68 — Схема подключения двухпортового зонда

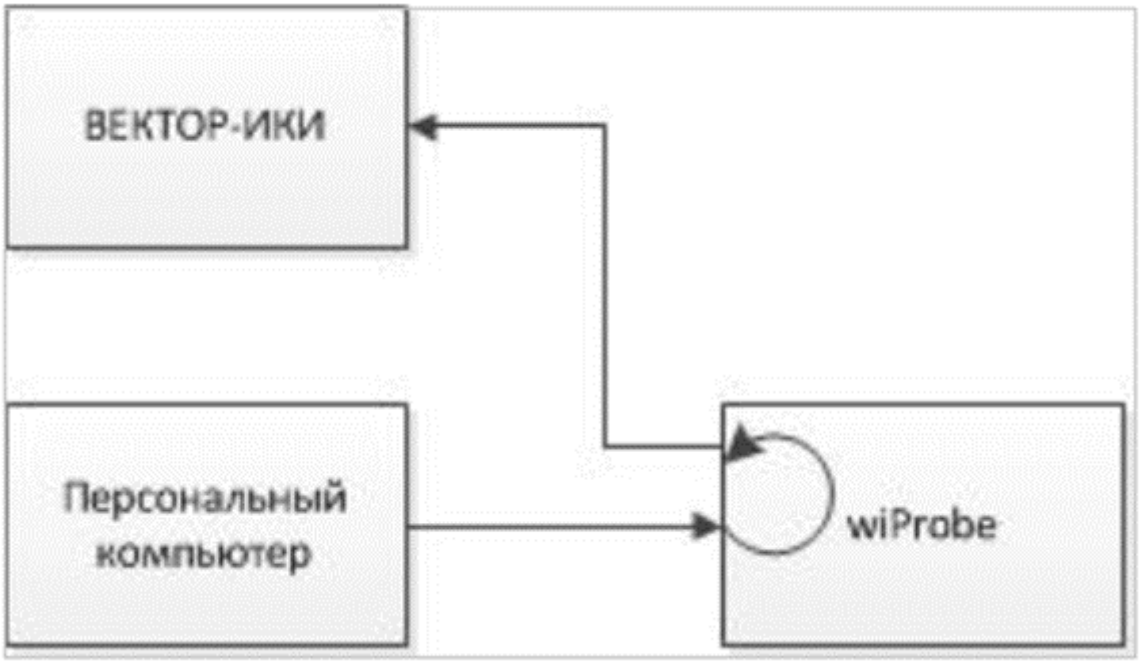


Рисунок 69 — Схема подключения однопортового зонда

Для двухпортовго зонда (Рисунок 67) необходимо ввести IP-адрес и порт назначения. Для однопортового зонда (Рисунок 68) — IP-адрес и порт назначения, а также локальный порт для зонда wiProbe, на который будут посылаться данные.

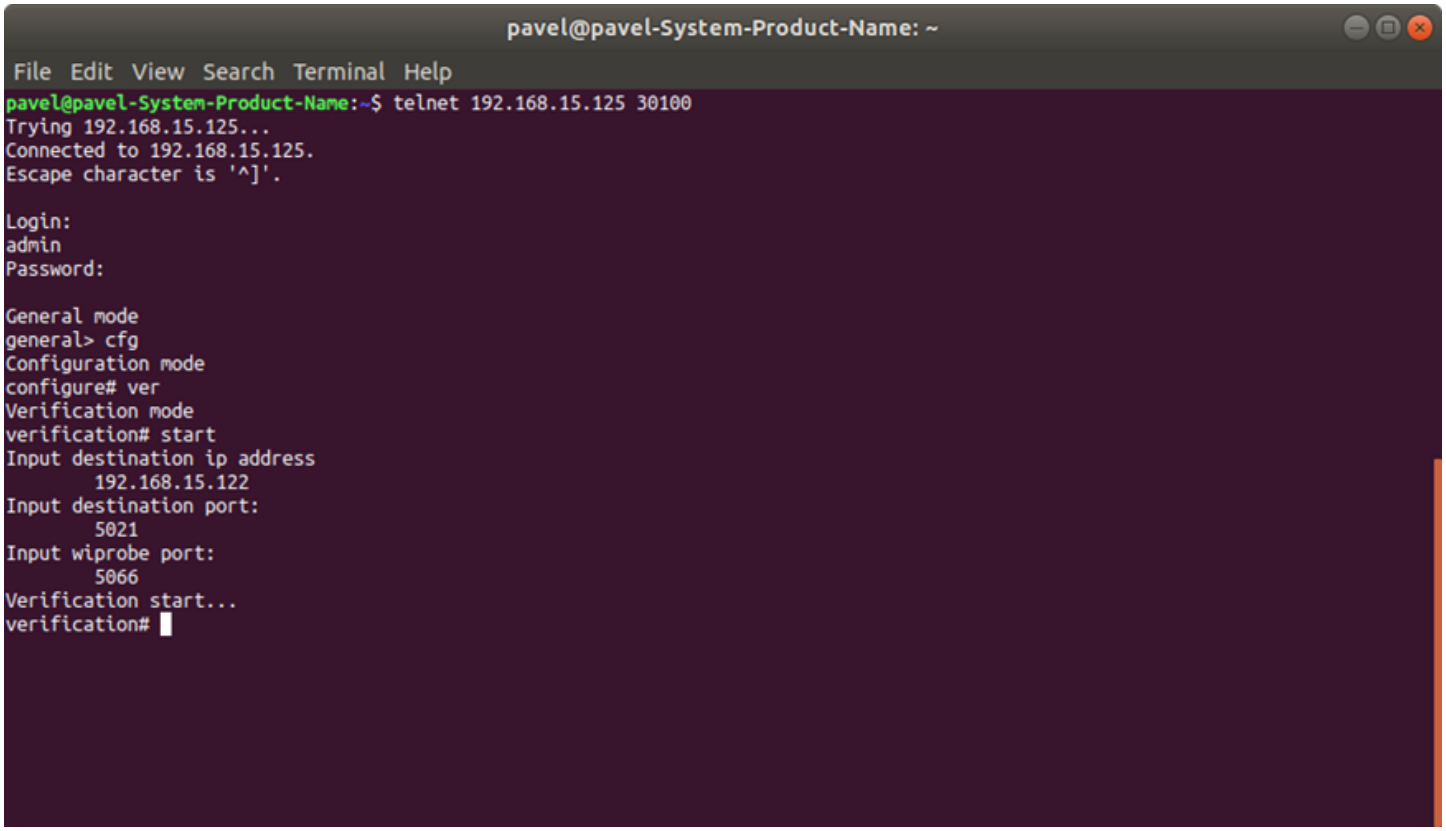


Рисунок 70 — Пример запуска поверки зонда

На рисунке 69 (схема собрана для однопортового зонда, как указано на рисунке 68) в качестве «Вектор-ИКИ» выступает хост с адресом 192.168.15.122:5021, у зонда wiProbe адрес 192.168.15.125. После ввода необходимых данных приостанавливается сетевая активность зонда и запрещается изменение данных из конфигурационного режима пользовательского telnet. Также сохраняется состояние iptables и добавляются новые правила для фиксации проходящего трафика.

Согласно схеме, персональный компьютер должен отправлять данные не напрямую «Вектор-ИКИ», а на порт 5066 зонда wiProbe. Зонд, в свою очередь, пересылает весь трафик, с порта 5066 на «Вектор-ИКИ», собирая необходимую информацию.

Пользователь, проводящий поверку зонда, в интерфейсе «Вектор-ИКИ» выбирает файлы эталонных размеров, которые будет передавать.

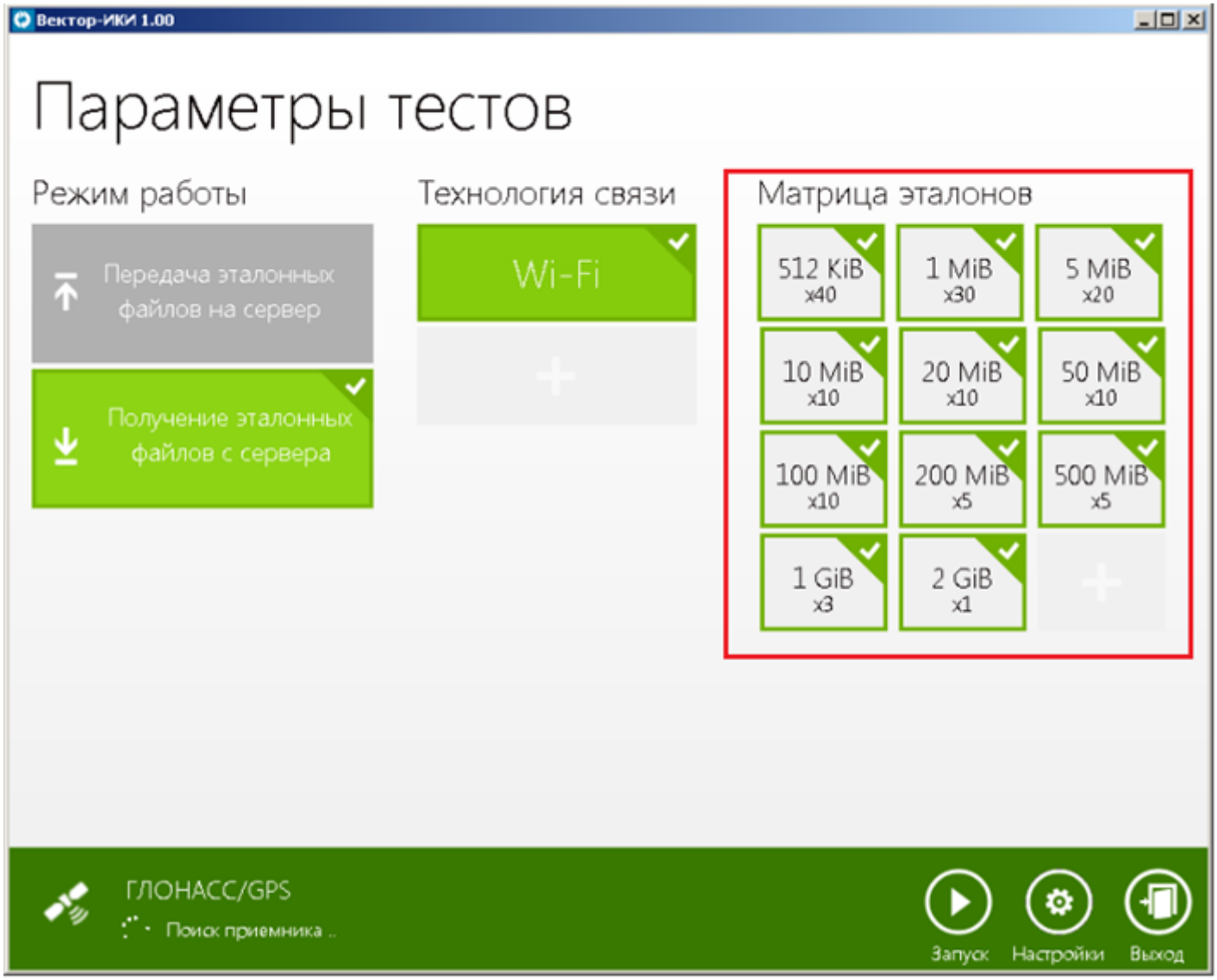


Рисунок 71 — Интерфейс измерительного комплекса «Вектор-ИКИ»,в котором выбираются файлы эталонных значений для передачи

После запуска измерительного комплекса «Вектор-ИКИ», в течение некоторого времени, осуществляется передача файлов с эталонными размерами. После окончания передачи, пользователю необходимо ввести команду `delim`, после которой произойдет подсчет следующих параметров:

- количество переданной информации;
- количество переданных пакетов;
- средняя скорость.

Для получения статистики по каждому переданному файлу необходимо передавать файлы по-одному и вводить команду `delim` после каждой передачи.

В качестве примера, будет запущена утилита «iperf», передающая трафик в течении заданного времени:

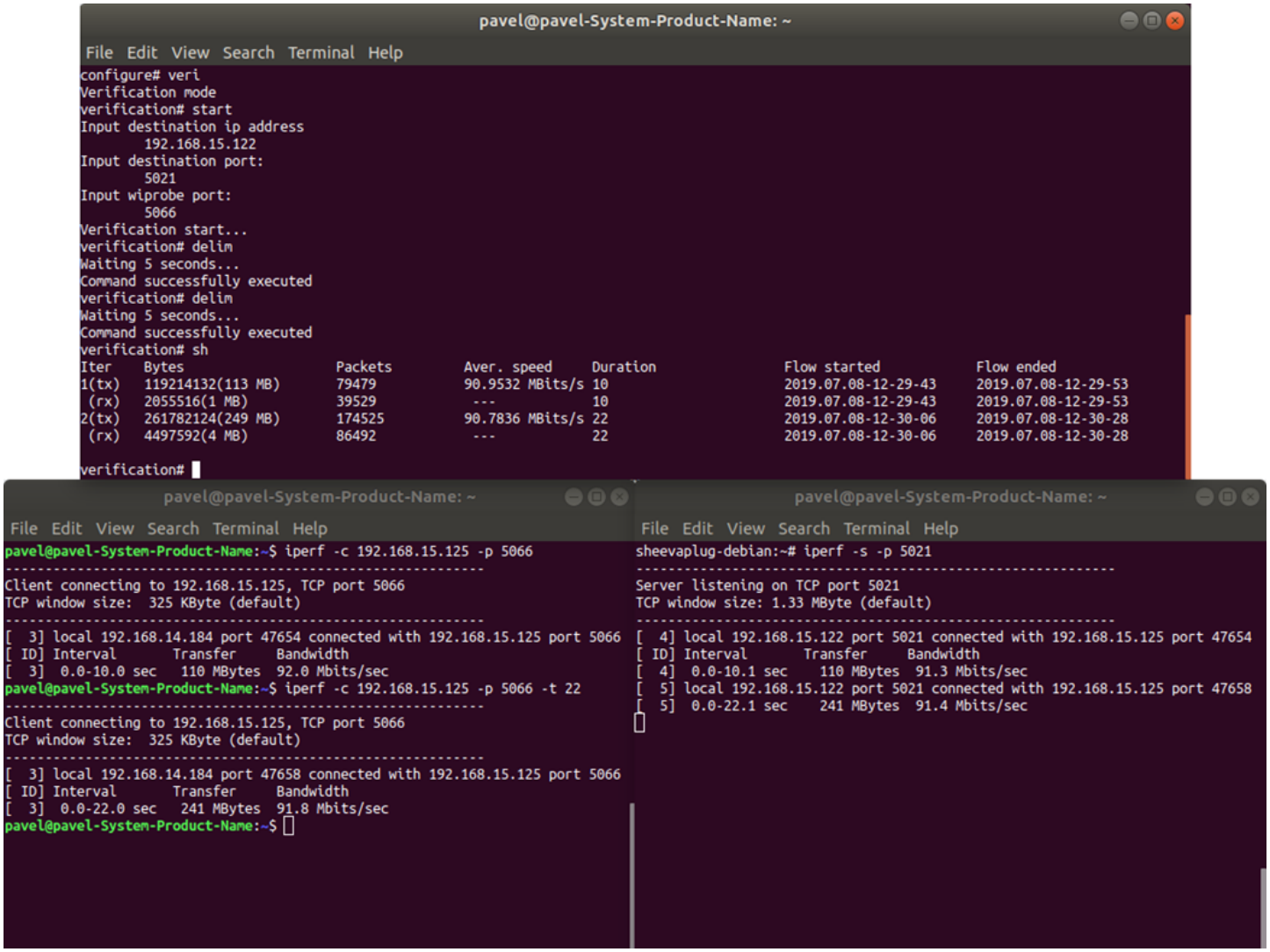


Рисунок 72 — Пример вывода режима поверки зонда wiProbe

Описание примера

В левом нижнем терминале запущен пользовательский telnet с зондом wiProbe (192.168.15.125). В правом нижнем терминале — зонд с адресом 192.168.15.122. Верхний терминал — это персональный компьютер на схеме.

Персональный компьютер (верхний терминал) генерирует трафик в течении 10 секунд на первой итерации, отправляя его на адрес 192.168.15.125:5066. wiProbe заворачивает его на адрес 192.168.15.122:5021 и анализирует. После того, как пройдет 10 секунд, вводится команда `delim`. Ожидание в течение 5 секунд, о котором сообщается в выводе, необходимо чтобы данные о нагрузке на сетевом интерфейсе передались в пространство пользователя. После чего, для просмотра результатов анализа проходящего потока данных, можно ввести команду `show`.

Формат вывода: Iter (номер файла, для которого выполнилась команда `delim`, подпись потока (прямой и обратный)), Bytes (количество переданных байтов), Packets (количество переданных пакетов), Aver. Speed (средняя скорость) и Duration (длительность передачи), Flow started (время начала передачи), Flow ended (время окончания передачи). На второй итерации iperf генерирует трафик в течение 22 секунд, затем все действия повторяются в telnet. Таким образом, каждый замер добавляется в вектор результатов.

Завершение поверки происходит с помощью ввода команды `stop`. Она возвращает iptables в изначальное состояние и восстанавливает сетевую активность устройства

Описание действий wiProbe при начале поверки

Команда `start`

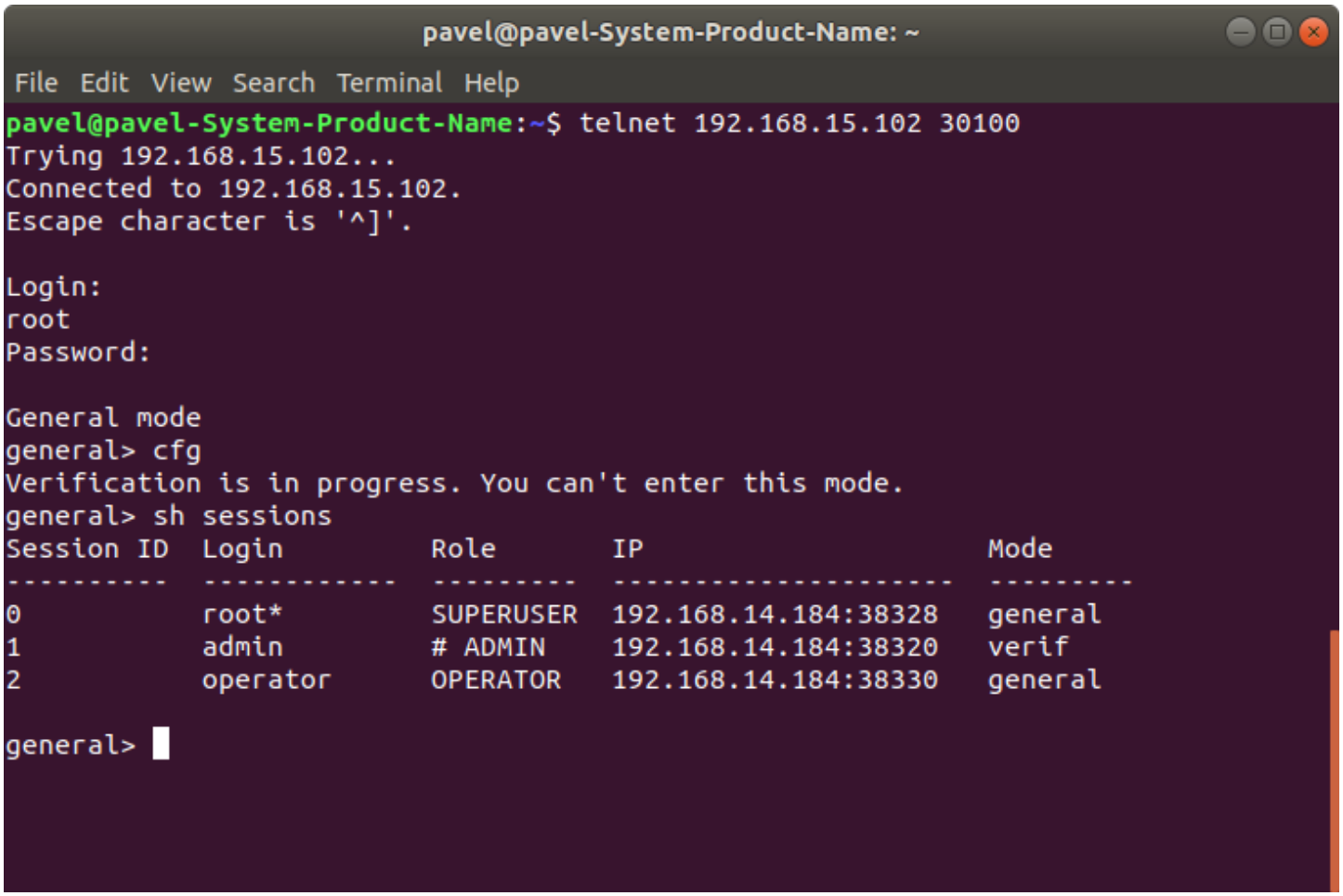
После получения команды `start` зонд сохраняет конфигурацию iptables, а затем добавляет новые правила. Для однопортового зонда:

iptables

iptables -t nat -A PREROUTING --dst 192.168.15.125 -p tcp --dport 5010 -j DNAT --to-destination 192.168.15.122:5011
iptables -I FORWARD 1 -i eth0 -o eth0 -d 192.168.15.122 -p tcp -m tcp --dport 5011 -j ACCEPT
iptables -t nat -A POSTROUTING --dst 192.168.15.122 -p tcp --dport 5011 -j SNAT --to-source 192.168.15.125
iptables -I FORWARD 1 -i eth0 -o eth0 -j ULOG --ulog-cprange 48 --ulog-qthreshold 50

В соответствии с приведенными правилами, все tcp-сегменты, пришедшие на порт 5010 зонда с адресом 192.168.15.125 будут перенаправлены на адрес 192.168.15.122:5011. Второе правило разрешает проброс пакетов на интерфейсе «eth0» к адресу 192.168.15.122. Третье правило подменяет адрес источника, чтобы пакеты также возвращались 125-му зонду, а не напрямую источнику. Четвертое правило копирует и передает в пространство пользователя первые 48 байт каждого пакета, накапливает информацию о 50 пакетах, прежде чем отправить информацию.

После этого отправляется команда модулю slamon, о приостановке сетевой активности (PAUSE_NETWORK_ACTIVITY) и захват блокировки сессией telnet. Другие пользователи не смогут войти в режим конфигурирования. Попытка войти в режим конфигурирования пользователем, обладающим блокировкой, переведет его обратно в режим верификации.



Символ «#» в столбце «Role», означает, что этот пользователь начал верификацию.

Команда `delim`

Каждая запись ulog-acctd имеет вид в соответствии с строкой форматирования (%s\t%d\t%S\t%D\t%b\t%P\t%x\t%t\n(из файла /etc/ulog-acctd.conf)):

account.log

source IP	dest IP	source port	dest port	bytes	packets	since	till
192.168.14.184	192.168.15.125	47658	7788	123151772	82105	1562037132	1562037142
192.168.15.125	192.168.14.184	7788	47658	3125337	32403	1562037132	1562037142
194.190.168.1	192.168.15.125	42832	123	76	1	1562037144	1562037144
192.36.143.130	192.168.15.125	55453	123	76	1	1562037146	1562037146
91.207.136.55	192.168.15.125	48632	123	76	1	1562037146	1562037146
194.190.168.1	192.168.15.125	47627	123	76	1	1562037176	1562037176
192.36.143.130	192.168.15.125	54658	123	76	1	1562037178	1562037178
91.207.136.55	192.168.15.125	51484	123	76	1	1562037178	1562037178

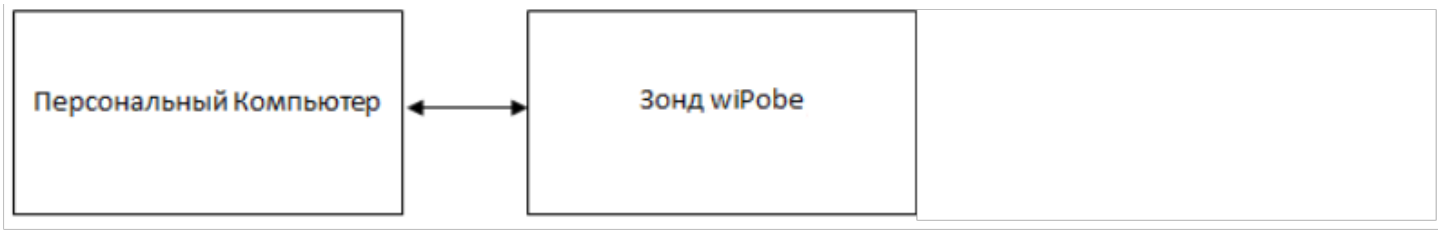
По адресу и порту назначения выбирается необходимый для анализа поток. Количество переданных байт, пакетов и длительность записываются в вектор. Поскольку время начала потока и окончания записывается в секундах, то существует следующая проблема: если начало передачи пришлось на ~0.96 секунды, а окончание на ~11.02 секунды, то доли секунды будут отброшены, и длительность составит 11 с, хотя на самом деле была 10.06 с.

Команда `stop`

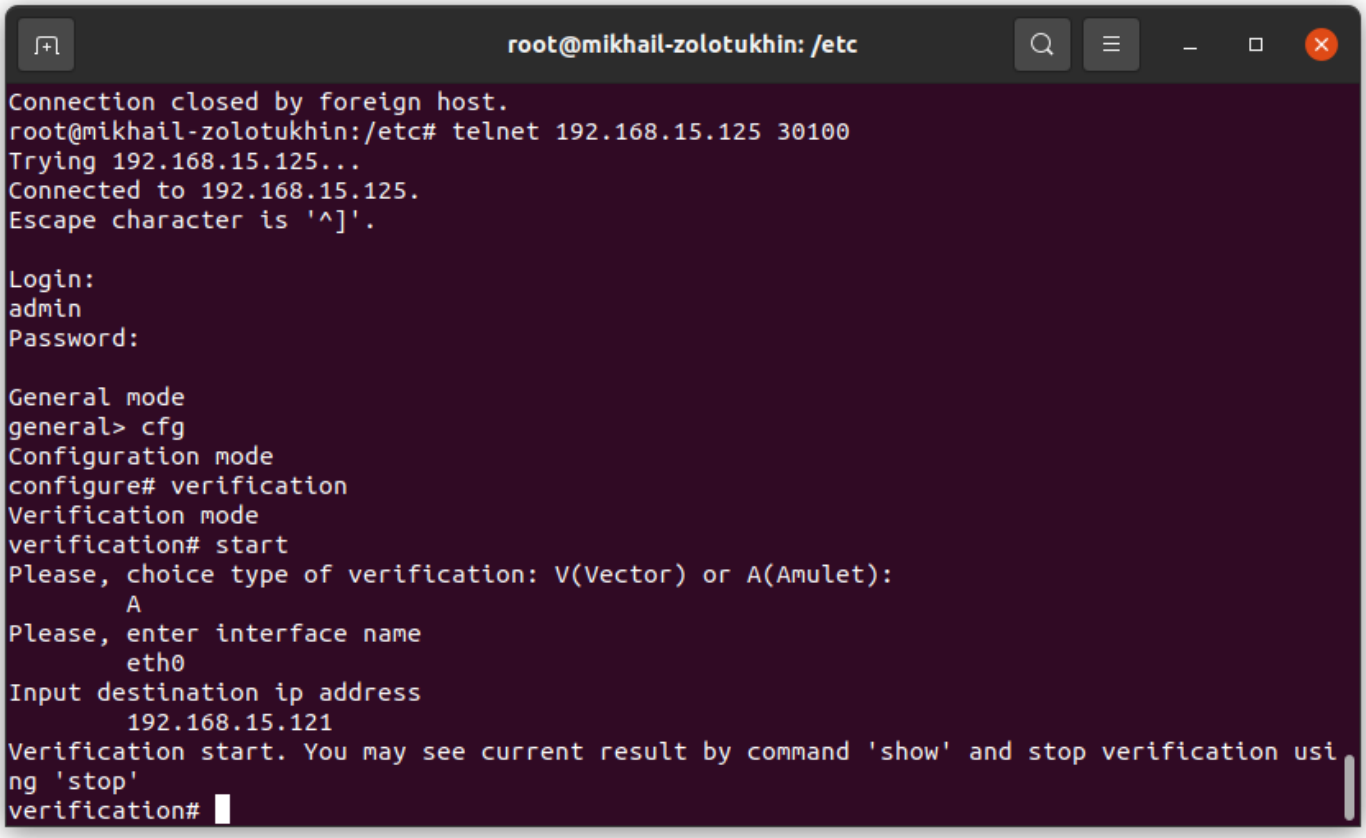
После этой команды зонд возвращает состояние iptables к тому, которое было перед началом поверки. Также выполняется команда восстановления сетевой активности (RESTORE_NETWORK_ACTIVITY).

Поверка с помощью "Амулет"

Схема:

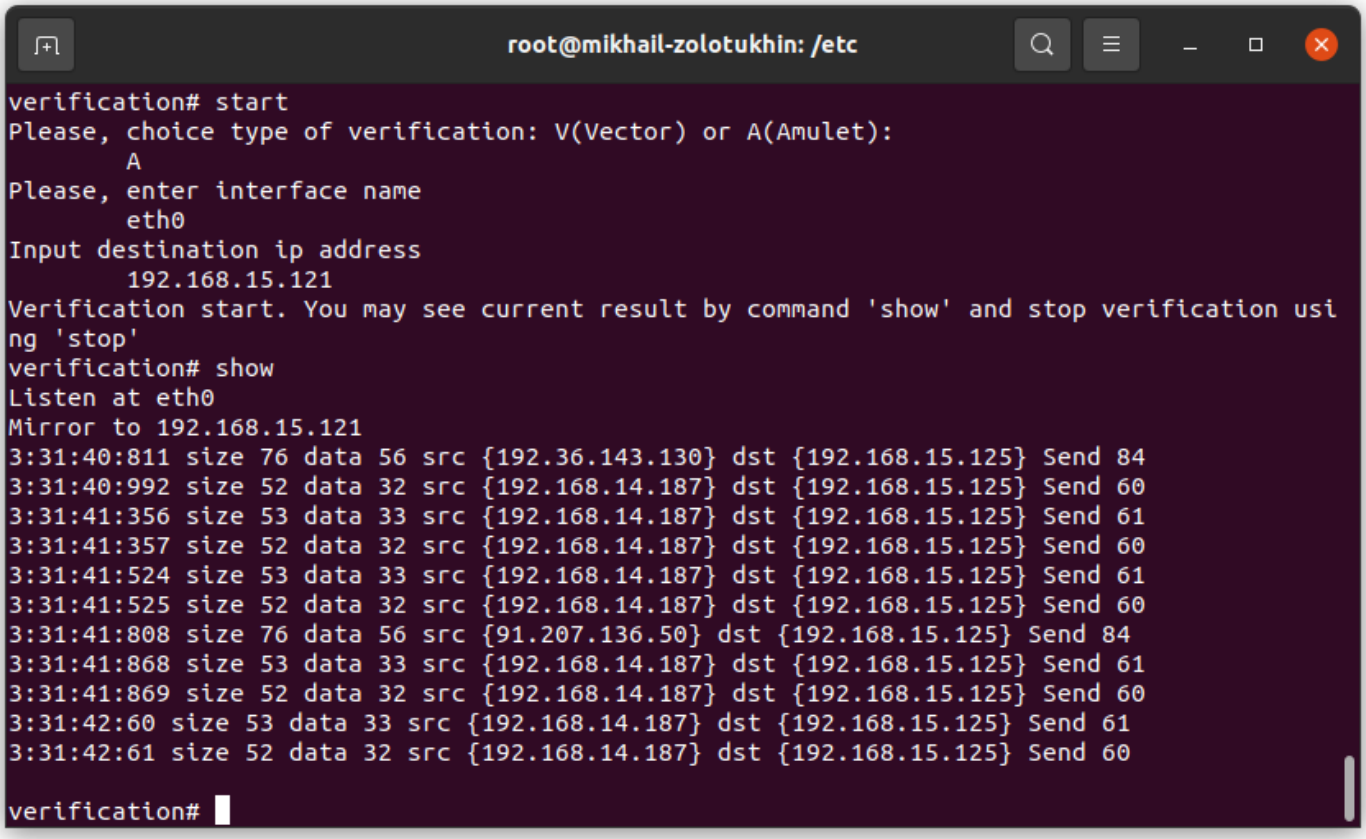


После ввода команды **`start`**, wizard запрашивает данные от пользователя и запускает процесс подсчета полученных и переданных данных



Команда `show`.

С помощью команды `show` можно посмотерть текущую статистику по полученным/отправленным данным.



Команда `stop`.

После команды `stop` текущая поверка заканчивается. Команда `show` после этого будет показывать статистку по прошедшей поверки.

Команда `exit`.

Делает выход из режима поверки.